Testimony before the
Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment
Committee on Homeland Security
United States House of Representatives

"Homeland Security Risk Assessments: Key Issues and Challenges"

November 17, 2005

A Statement by

Christine E. Wormuth
Senior Fellow, International Security Program

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, 1800 K STREET, NW, WASHINGTON, DC 20006
TELEPHONE: (202) 887-0200; FACSIMILE: (202) 775-3199 WWW.CSIS.ORG

Mr. Chairman, Ranking Member Lofgren, members of the subcommittee, thank you for inviting me to testify before you today on assessing the risks of terrorism.

Assessing homeland security risks, which can stem from both terrorism and natural disasters, is an enormously complex undertaking but is also a critical task if the federal government seeks to marshal its finite resources effectively. Before turning to the key policy issue of how to use risk assessments to maximize unity of effort at the federal level, I would like to briefly outline what makes a basic risk assessment and some of the challenges inherent in trying to assess homeland security risks.

As Secretary Chertoff has emphasized since being named Secretary of Homeland Security, focusing on the "trio of threat, vulnerability and consequence as a general model for assessing risk" is at the heart of the DHS approach. It is worth peeling back the layers of the onion in those three areas a bit more fully to understand the complexities associated with assessing homeland security risks.

In most formal discussions of risk assessment, risk is defined as the product of the probability that a certain event might occur — a suicide bomber attack on a hotel such as we saw take place last week in Jordan — and the consequences that could result from such an event. The probability side of the equation is basically a combination of threats and vulnerabilities. Threats could be assessed in terms of the different kinds of weapons and delivery systems that might be available to our enemies. In some cases weapons could be relatively difficult to acquire or develop, like the smallpox virus or a small nuclear device, or they could be much more common — an improvised explosive device carried on a delivery truck. Assessing vulnerabilities means establishing the pool of possible targets — which could include buildings that are vulnerable every day like chemical plants or once-a-year events like the Super Bowl — and determining how vulnerable they are to the full range of threats. The final piece of a basic risk assessment involves looking at the consequences that might result from different attacks. Consequences might include not only the deaths and injuries that could result, but also the economic and psychological costs of a given type of attack, and the length of time it takes to resume normal activity levels after the attack.

The basic formula for a risk assessment is simple — probability times consequences equals risks — but in practice assessing homeland security risks poses some important practical challenges.

One challenge is the lack of quantitative data on which to base assessments of probability and consequences. We cannot determine the probability of terrorist attacks — the "percent chance" that a specific type of attack might occur. Nor do we have extensive quantitative data to pinpoint the numbers of potential fatalities or economic costs that might be associated with particular kinds of attacks. And how should we begin to think about psychological consequences? Can they be expressed quantitatively? We can use expert judgment and computer models to extrapolate representations of probability and consequences but they will be just that - representations rather than certainties.

Another challenge is how to handle intelligence. Many of you on the committee have noted the importance of intelligence in developing homeland security risk assessments. But determining how to incorporate intelligence effectively is a challenge for analysts. How can DHS develop models that factor in specific intelligence we may have about particular targets or payloads without skewing an assessment toward only those risks on which we have intelligence? As Secretary Rumsfeld has often said, "we don't know what we don't know," — just because the

intelligence community does not have information that suggests a terrorist group has a WMD capability does not mean that group doesn't have a WMD capability. Or vice versa.

Whether to weight the different pieces of a risk assessment is another challenge. Should some kinds of targets be weighted more heavily if we know groups like Al Qaeda have expressed the intention to attack them? Should human deaths be weighted more heavily than other types of consequences? By how much?

Despite these formidable challenges, it is absolutely worth the time and effort to develop robust homeland security risk assessments that can guide our planning and policy development. Risk assessments – even if they are based on imperfect intelligence, expert opinion, and computer simulations of potential consequences – give us the tools to examine many different pieces of complex information in a structured way. They focus attention on the specific judgments that cumulate into an overall risk ranking and hence they can be "unpacked" to better understand where differences of opinion may lie and how they affect the assessment. Policy makers can use the structure that risk assessments provide to understand clearly where there are disagreements in the expert community, and can then assess for themselves the different sides of the debate before coming to a policy judgment that may have profound implications down the road.

DHS would serve all of the Cabinet agencies with homeland security responsibilities well by taking the lead in developing a "National Homeland Security Risk Assessment" that would assess and rank the full spectrum of plausible homeland security risks — an assessment that would look comprehensively across all of the kinds of critical infrastructure and other potential target types combined with the different weapon payloads and delivery systems that adversaries might seek to use against the United States. As this Committee knows well, the legislation that established DHS stipulated that the department would develop a comprehensive risk assessment. This assessment is still of paramount importance.

This type of assessment, much like a National Intelligence Estimate, would be developed on a regular basis, perhaps every couple of years, and would serve as the authoritative assessment of homeland security risks, identify trends of significance for homeland security and if necessary, identify differences of views about risks among the principal senior leaders in the U.S. government homeland security arena. Development of a National Risk Assessment should be an interagency undertaking, with DHS in the lead, but with significant support from the broader intelligence community, DoD, HHS, the Department of Energy, other Cabinet agencies, and leaders from the private sector and industry. A National Risk Assessment would sacrifice examining the threats, vulnerabilities and consequences of every possible scenario in their fullest details for a process that could generate actionable results in the near-term, at least in terms of setting broad priorities and directions. Subsequent, more detailed risk assessments focused on specific threats or infrastructure sectors could then fill in the details over a longer period of time.

A National Risk Assessment could strengthen the homeland security policy development and resource allocation process in at least three very important ways.

- Guiding homeland security planning. As CSIS noted in its recently released *Beyond Goldwater Nichols Phase II* report, before the interagency can develop robust concepts of operations for homeland security, it needs to conduct a strategic risk assessment. A National Risk Assessment would not only serve as the basis for developing common interagency strategies for addressing specific homeland security challenges, it would also serve as the basis for developing national homeland security planning scenarios. Putting forth the fifteen Homeland Security Council scenarios was an important step toward

harmonizing ongoing planning activities, but those scenarios could play a larger role in driving policy, planning, and programming if they were based on the results of an interagency-agreed National Risk Assessment.

- Driving the resource allocation process. Many have noted the importance of using risk assessments to set broad priorities for how DHS allocates resources. Looking beyond DHS, a National Risk Assessment could serve as the basis by which to harmonize not just DHS resource and policy decisions, but homeland security related resource and policy decisions across the entire interagency. This would go a long way toward creating maximum unity of effort across the USG in this critical area.
- Evaluating potential policy and programmatic options. Where should DHS and other agencies invest their marginal dollars? What will give us more bang for the buck, ten more bomb detector dog teams, 50 more handheld radiation detectors, or 100 more border patrol agents? These are the kinds of real world decisions DHS and other agencies have to grapple with in their budget processes, and risk assessment tools can help shed light on these choices in a structured way.

Secretary Chertoff has asked Congress for the authority to establish an Under Secretary for Policy in DHS. This is a very important and much needed position, and it is good news that Mr. Stewart Baker was confirmed earlier this year at the Assistant Secretary level. In my view, one of his central responsibilities should be to lead the development of a National Risk Assessment, working closely with his peers in the other relevant Cabinet agencies, and then to institutionalize the results into DHS's broader strategic planning and resource allocation processes. The Under Secretary, with his direct access to Secretary Chertoff, can elevate and integrate the many useful risk assessment processes ongoing inside DHS to help build a coherent, comprehensive risk assessment picture that truly drives policy and programming at the strategic level. In *DHS 2.0, Rethinking the Department of Homeland Security*, my colleague David Heyman at CSIS and James Carafano of the Heritage Foundation called on DHS to deliver a comprehensive risk assessment to our top national security leaders by December 2006. I think this remains a reasonable deadline. Highly granular assessments will clearly be needed, and there are assessment tools in development that will help us make finely tuned adjustments to our prevention, response and preparedness programs over time. But today, more than four years after the September 11 attacks, we need a comprehensive National Risk Assessment — and we need it soon. That means senior leaders, in the Executive branch and here in Congress, will have to make choices and set priorities on less than perfect information. That said, I suspect most Americans would prefer to see the government make those tough choices rather than letting the best be the enemy of the good. I applaud this Committee for engaging on this issue and thank you for the opportunity to share my views.